TECHNICAL SECURITY ASSESSMENTS

Validate Implementation and Security Configuration of your IT Systems

Overview

A Technical Assessment provides you with an understanding of the security posture of an IT system with a specific focus on validating security functions, including technology that has already had security hardening.

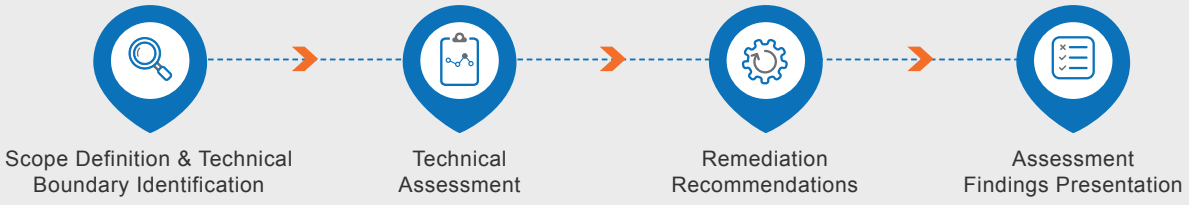
Technical Assessments can also include validating the implementation of technical controls under industry or government frameworks, such as the Australian Cyber Security Centre's (ACSC) hardening guides.

A Technical Assessment will provide you with a report outlining the systems assessed and detailing security issues identified and recommended remediation activities.

> *" Security is an on-going process, and as an IT Security Advisor, I am comfortable with having a peer company like Shearwater to rely upon. If I have an issue or need advice I am confident that Shearwater can provide a pragmatic and cost-effective solution. "*
>
> ITSA, Federal Government Agency

How it Works

A technical assessment has a four-step lifecycle:



1. Scope Definition & Technical Boundary Identification

Prior to conducting the assessment, we start by defining the scope and technical boundaries. We specifically look at the system architecture, data flows, connections with other systems, any remote access capabilities, and the physical location of infrastructure and technologies used. This information is then used to define and agree on a technical boundary for the assessment.

Where there is a requirement for the technical assessment to include validating system configuration against an industry or government standard, we will define the scope and technical boundaries based on the requirements of that specific standard.

2. Technical Assessment

During the assessment stage, we will work with your engineers, architects and DevOps personnel to conduct a technical implementation review.

We will review and validate system configuration. This step requires evidence-based testing and we will leverage different tools to validate that the implementation and configuration of your systems are effective.

At this stage, we will - if relevant - identify gaps in meeting security best practice, industry or government requirements.

3. Remediation Recommendations

During this stage, the focus will be on improving the overall security posture of the system(s) being assessed with special attention to the areas where specific security weaknesses were identified.

Depending on the scope of the engagement, this may include identifying remediation activities that follow industry or government guidelines or standards. Remediation recommendations may be technically prescriptive or alternatively focus on providing advice on the different ways to meet the intent of a relevant security control from a standard.

The identification of remediation activities also considers defence-in-depth provided by the system being assessed and other related systems.

4. Assessment Findings Presentation

Based on the information and evidence collected, we will prepare a draft report detailing the technical scope, identified security issues and recommended remediation activities. If required, we will seek additional information to clarify understanding and ensure that the report aligns with expectations and requirements.

Then, we present the findings outlined in the draft report, covering the key security issues identified and recommended remediation activities for key stakeholders. This provides an opportunity to gather client feedback and ensure expectations have been met before issuing a final report.

Summary Presentation for C-Suite & Board Members

This optional presentation of findings to key executives helps to align your security initiatives with your organisation's business goals and overall risk management strategy. This session provides senior executives with jargon-free digestible information around the Technical Assessment findings and enables them to ask questions and voice any concerns. By forging an understanding of security threats as they manifest on a business level, this presentation is useful in justifying security spend and getting buy-in for further budgetary requirements.

About Shearwater

Shearwater is a specialist information security service provider with an unwavering focus on providing service excellence across our portfolio of services. Since 2003, we have enabled millions of secure interactions across government and private sectors.

Shearwater's expertise include security education, security operations management, security consulting, and application security including penetration testing. Our highly developed methodologies enable organisations to implement best security practices and help them achieve, maintain and prove compliance against a range of security standards.

Shearwater focuses on helping you manage the security risks associated with running your business whilst providing actionable recommendations to the internal security team. We pride ourselves on client communication, customer service, fast response, and on-time delivery.

Shearwater is part of the CyberCX group - Australia's leading independent cyber security services company.

WHATEVER YOUR INFORMATION SECURITY CHALLENGE, WE'RE HERE TO HELP YOU FIND THE RIGHT SOLUTION.

www.shearwater.com.au 1300 228 872

Sydney | Melbourne | Canberra | Brisbane | Perth